Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A secure on-line system for printing value bearing items (VBI) comprising:

a client system ~~for interfacing~~ configured to interface with a plurality of users; and

a server system ~~for communicating~~ configured to communicate with the client system over a communication network comprising:

a secure database remote from the users including a data record for each of the users; and

a plurality of stateless cryptographic ~~modules~~devices, each of the plurality of stateless cryptographic ~~modules for authenticating~~ devices configured to perform authentication, processing value for the VBI, and ~~generating~~ generation of indicia data for the plurality of users, wherein before each of the authentication, processing value, and ~~generating~~ generation of indicia data for a given user is performed, an available cryptographic ~~module~~device in the server system retrieves the data record for the given user directly from the database, and wherein after the authentication, processing value, and generation of indicia data are performed, the client system instructs a printer to print the VBI.

2.-4. (Cancelled)

5. (Previously Presented) The secure on-line system of claim 1, further comprising computer executable code for an asynchronous dynamic password verification to terminate a user session if the password authentication fails.

6. (Currently Amended) The secure on-line system of claim 1, wherein the database stores a first set of one or more last database transactions and each of the cryptographic ~~modules~~

devices stores a second set of one or more last database transactions for comparison with the first set of one or more last database transactions stored in the database to verify each database transaction.

7. (Currently Amended) The secure on-line system of claim 6, wherein each of the cryptographic ~~modules~~ devices prevents further database transactions if the second set of one or more last transaction stored in the cryptographic ~~module~~ device does not match with the first set of one or more last transaction stored in the database.

8. (Previously Presented) The secure on-line system of claim 6, wherein the database stores a table including the respective information about a last transaction and a verification module to compare the information saved in the module with the information saved in the database.

9. (Previously Presented) The secure on-line system of claim 1, further comprising a back up database server connected to the server system for periodically backing up the data stored in the database in a back up database.

10. (Previously Presented) The secure on-line system of claim 9, further comprising a cryptographically protected transaction log stored in the back up database.

11.-16. (Cancelled)

17. (Currently Amended) The secure on-line system of claim 1, wherein each of the cryptographic ~~modules~~ devices includes a data validation subsystem to verify that data is up to date and an auto-recovery subsystem for allowing the ~~module~~ device to automatically re-synchronize the ~~module~~ device with the data.

18.-21. (Cancelled)

22. (Currently Amended) The secure on-line system of claim 1, wherein each of the cryptographic ~~modules~~ devices includes a computer executable code for detecting errors and preventing a compromise of data or critical cryptographic security parameters as a result of the errors.

23.-41. (Cancelled)

42. (Previously Presented) The secure on-line system of claim 1, wherein the server system further comprises one or more of a postal server subsystem, a provider server subsystem, an e-commerce subsystem, a staging subsystem, a client support subsystem, a decision support subsystem, a SMTP subsystem, an address matching service subsystem, a SSL proxy server subsystem, and a web server subsystem.

43.-49. (Cancelled)

50. (Currently Amended) A method for securely printing value-bearing items (VBI) via a communication network including a client system, and a server system including a plurality of stateless cryptographic ~~modules~~devices, the method comprising the steps of:

interfacing with a plurality of users remote from the plurality of stateless cryptographic devices, via the client system;

communicating with the client system over the communication network;

storing a data record for each of the plurality of users in a database remote from the plurality of users;

directly retrieving the data record for a given user from the database for authenticating the given user, processing value for the VBI and generating indicia data for the given user, by any available cryptographic ~~module~~device of the plurality of stateless cryptographic ~~modules~~devices; and

updating the data record[[,]] and storing ~~in the database,~~ the updated data record for the given user in the database; and

printing the VBI by the client system.

51. (Currently Amended) The method of claim 50, further comprising the step of encrypting each database transaction ~~by a cryptographic module~~.

52. (Currently Amended) The method of claim 50, further comprising the steps of

storing one or more last database transactions in the database;

storing one or more last database transactions in [[a]] the cryptographic ~~module~~ device; and

comparing the one or more last database transactions stored in the database with the one or more last database transactions stored in the available cryptographic ~~module~~ device to verify each database transaction.

53.-54. (Cancelled)

55. (Currently Amended) The method of claim 50, further comprising the steps of storing one or more last database transactions in the database, storing one or more last database transactions in the available cryptographic ~~module~~ device for comparison with the one or more last database transactions stored in the database to verify each database transaction.

56. (Currently Amended) The method of claim 55, further comprising the step of preventing further database transactions if the one or more last transaction stored in the cryptographic ~~module~~ device does not match with the one or more last transaction stored in the database.

57. (Currently Amended) The method of claim 50, further comprising the step of storing a table including the respective information about a last transaction and comparing the information saved in the available cryptographic ~~module~~ device with the information saved in the database.

58. (Original) The method of claim 50, further comprising the step of backing up data stored in the database in a back up database.

59. (Original) The method of claim 58, further comprising the step of recovering data from the back up database by decrypting an encrypted transaction log stored in the back up database.

60.-121. (Cancelled)